Introduction

The University of Illinois Information Security Policy is a University-wide policy on the use of data, applications, networks and computer systems. This policy on Administrative Information Security provides further guidelines for the financial, human resource and student systems at the University of Illinois. In this policy, “systems” are broadly defined to include the application software, the supporting hardware, and the support personnel.

Responsibilities

Information User

Anyone accessing University administrative information assumes a fiduciary responsibility and is therefore obligated to preserve the security and confidentiality of the information. Such information is to be used only for conducting University business, or as otherwise authorized by University Administration.

Faculty, staff and students are expected to exercise responsible, ethical behavior when using the University's computers, information, networks or resources for administrative information management purposes. Individual responsibilities include preserving the confidentiality and security of data to which they have been granted access and ensuring that data are used for and in the conduct of University business. These responsibilities include the proper storage, access, control, dissemination and disposal of high risk and confidential data presented to the user in any form. Personal or unauthorized use of systems and/or data is prohibited. Individuals must also report known or suspected security violations to the Associate Vice President for Administrative Information Technology Services or his delegate, who will be responsible for contacting other relevant University offices (legal, HR, etc…).

Data Custodian

The University has delegated operational data control to various University colleges, units and affiliated groups known as Data Custodians. Data Custodians, are authorized to grant access permission to data maintained by them to staff in other University units when necessary for the efficient management of the University. Their responsibilities include:

?? Authorizing access to data.
?? Interpreting pertinent laws and University policies which determine the levels of confidentiality and security required for data.
?? Aiding users in accessing and interpreting data.
?? Providing guidance to the AITS Information Security Officers in establishing appropriate levels of security and confidentiality.
?? Reviewing security violations.

The term "data" is a general term used to describe facts, numbers, letters and symbols that refer to or describe an object, idea, condition or situation.

Supporting Units

Any unit supporting servers on which business information resides must implement the Data Custodian access authorization described above and maintain system security functions as outlined in this section. Each unit must:

?? Implement data security policies and standards that are consistent with the University Information Security Policy.

?? Assure compliance for each system that falls within the scope of its direct responsibility.

This includes development and maintenance of an internal security plan and associated documents which assure data integrity, authentication, recovery and continuity of operations which support administrative data. It also includes such details as type of access controls, disaster recovery plans and contingency plans for continuous operation in case of power outages, etc. These documents are considered a part of the policy statement.

Office of University Audits

The University's internal auditors are authorized for inquiry-only access to all administrative information and systems. Internal auditors are responsible for:

?? Evaluating University departments for compliance with information security policy and procedures during operational and administrative audits.

?? Evaluating the effectiveness of security procedures and other internal controls.

?? Reviewing audit trails provided by System Administrators to determine whether activity is adequately documented.

?? Assisting management in the investigation of suspected incidents of security breach or improper activity.

?? Providing advice regarding internal controls.

Ownership

The University of Illinois owns all information (data, programs and procedures) gathered, stored or maintained for business purposes, unless otherwise stated in a contractual agreement. This ownership includes all forms of the information—electronic or printed. It includes all copies of information on mainframe, mid-range and personal computers, and local area networks, wherever the equipment or networks are located.

Violations

Violation of any provision of this Policy includes but is not limited to the University taking the following actions:

?? Limiting the individual's access to some or all University systems.

?? Enforcing disciplinary sanctions in accordance with the relevant University policy as outlined in:

University Policy and Rules for Civil Service Staff
University of Illinois Statutes (February, 1994)
Academic Staff Handbook
Code on Campus Affairs

?? Initiating legal action, including, but not limited to, criminal prosecution under appropriate state and federal laws.